Public–Private Key Cryptography Based Secure Identity and Transaction Management in Blockchain

Asif Mulla*[1], Dr. Arunkumar Joshi*[2], Rashmi P.C *[3], Deeksh K R*[4]
*[1]*Department of Computer Science and Engineering, Alva's Institute of Engineering & Technology,* -Moodabidri India
*[2]*Department of Computer Science and Engineering, SKSVMACET,* Laxmeshwar-India
*[3]*Department of Computer Science and Engineering,* Vivekananda College of Engineering & Technology, Puttur, India
*[4]*Department of Information Science and Engineering, Yenepoya Institute of Technology* –Moodabidri India

Abstract: **A Blockchain is a new type of applications and solutions for identity management, trust, and data monetization. Blockchain is fundamentally a conveyed database of records or digital occasions that are executed and shared among taking an interest parties. The most theory is that the blockchain provides the basis for a collective consensus in the electronic digital environment. It opens the entryway for creating a majority rule open and versatile advanced economy from a centralized one. Blockchain is that the technology backbone of Bitcoin. The blockchain provides a complete and testable database of any single exchange that's ever been generated. Bitcoin, the digital money anonymous peer-to - peer, is the latest indication that utilizes blockchain technologies.The explanation bitcoin's going to be disturbing beginner point is which mathematic work and innovation behind it redefines the construct of possession. This paper purposes the mathematical solution behind Blockchain technology and created a few instinct regarding the mathematical relationship that exists between public and private keys get to a private-key & public-key ECDSA combination is essence of how Bitcoin and other apps of blockchains work. The ECDSA takes isolated strategies for signing, verification as well as confirmation. Every method it such calculation comprising a few mathematical functions of numbers. The able to sign algorithm makes use of private-key & public-key is utilized during confirmation process.**

Keywords: Blockchain, Bitcoin, Hashcode, ECDSA, Digital Signature, Private Key, Public key, Point, Curve.

I. INTRODUCTION

Blockchain is one of the most recent developments that have made more consideration over the last few a years. The blockchain technology refers to any account of digital assets traded digitally. Blockchain contains a definite and verifiable transaction record which has forever been complete. This innovation is essentially a disseminated file of records or advanced occasions that are performed and exchanged between recorders. Blockchain can be described as a linked data block chain that allows transaction records to be generated on the basis Of like a decentralized, participant-controlled shared ledger lacking a central authority. Throughout the easiest of quotes, a blockchain can be a time-stamped set of unchanged data records that is maintained by an organization of machines that no one works.. All of such data bricks (ie-blocks) is guarded to use the concepts of cryptography (ie-chain) and linked together. Building, the record-chain is unchangeable; this is nope single hub can switch quality of blocks previously approved. Blockchain is the Bitcoin's core of technology.

Bitcoin could be a virtual cash. This means it exists only digitally, it has no physical notes or coins, and it can be used to buy items on the internet. Some of the keys reason people would choose to use Bitcoin is that it operates globally, and is not regulated by any government or corporation. It can be very beneficial because several companies are now working online, and are trading in many countries. Companies and individuals who move between currencies want to stop charging trading fees and taxes. They don't need to pay any of those charges with a digital currency like Bitcoin. Bitcoin is the most common example of blockchain technology inherently tied to. Blockchain is a freely open ledger on which users utilized a Elliptic Curve Digital Signature Algorithm (ECDSA) to submit details and verify transaction approval. Elliptic-curves are a really vital modern zone of science which has been significantly investigated over the past few decades. They showed enormous potential as a method for solving complex problems with numbers and also for use in cryptography. An elliptical curve cryptography could be a sort of public key cryptography, depending on arithmetic to guarantee that an exchange is secure. Maths is keeping your information secure. Elliptic curve cryptography, fair as RSA cryptography. The fundamental thought behind this is often that of a lock.

II. RELATED WORK

It is generally recognized that certain mathematical problems in cryptography, blockchain and information security work played indispensable roles.

The foremost cryptographic tools related to blockchain protection and security are shown: Digitalsignature, hash functions, elliptic-curves. The digital-signature calculation utilized by numerous blockchain innovations Is ECDSA, the specification used in elliptic curve. Many implementations have selected sep256k1 from among all the curves that can be included. Secp256k1 can be an elliptical foundation bent with 256-bit key, a level of quality compared to the code AES [3]. The suggested online communication system, without relying on the assumption. We began also with a standard scheme of digitally signed coin, that provides strong owner protection but is insufficient without any of the likelihoods of preventing dual expenditure.We introduced the peer-to-peer network worked evidence of research to document an transparent background of transactions that would easily become algorithmically irrational if real nodes were to manage a greater portion of the CPU power [4].

Using blockchain, we used common business applications to handle the building details as files. Instead of enormous scale of BIM data, with restricted management capabilities the usability of such versions few options. The proper location for blockchain Inclusion is with the BIM Database part of the transaction collection and its management functions. Moreover, Fingerprints or chaining of all such computer exchanges and correspondence will be blockchain [5]. The blockchain innovation along with a few

of its important focal points. For a number of fields for various areas and sectors, the technology is always evolving, and is likely to change the direction the world is going. But it is not free of challenges, some of which have already been highlighted [6]. A technical overview of blockchains through a review of their key technical functions and an analysis of their possible applications for industry. As illustrated, current and potential developments focused on blockchain cover a variety of uses and industries beyond the digital currency and the economic field [7]. The latest summary on blockchain is detailed. We to begin with the offer an diagram of blockchain innovation like blockchain design as well as main blockchain characteristics. The standard acceptance algorithms used in blockchain are discussed then. We evaluated these protocols and compared them in distinctive regards also identified more Challenges as well as difficulties inhibit the growth of blockchain and described some current approaches to solving these problems [8].

Miners-Miners Hide their mined blocks in the future, used for additional income. Therefore, branches may frequently take place which hinder Technology to blockchain. And certain ideas must be put in place Go ahead to fix the problem. In fact, it was shown that Security leakage in blockchain may also occur to users Enable only transactions with its pub-key and private-key [9]. The view of this paper is the importance of a certain mathematical issue, which has associations to the major subject blockchain and Bitcoin.

III. TECHNOLOGY OF BLOCKCHAIN

The blockchain is an evidently brilliant innovation – the brainchild of an individual or gather of individuals known by the pseudonym, Satoshi Nakamoto[4]. A blockchain is basically a chain of squares that contains data. Every block of hash code, timestamp and transaction details of the previous block. Despite its simplistic architecture, it is this complexity that renders Blockchain invulnerable to information altering.

A. Blockchain Working Process:

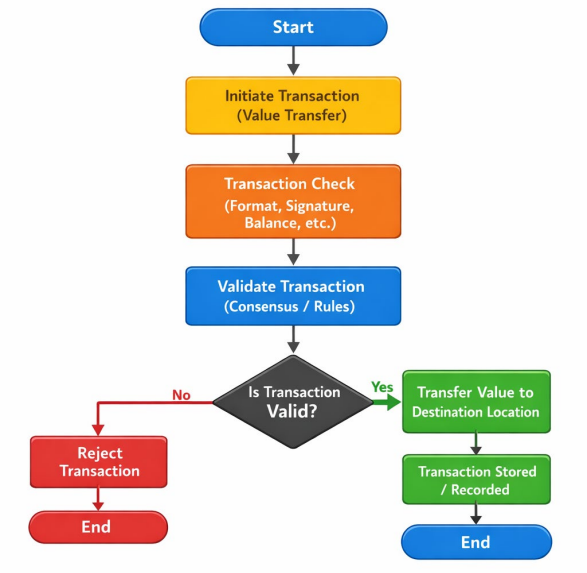

Fig. 1. The values can only be passed to another location when the transaction is checked and validated.

Blockchain is usually worked by a peer-to-peer organize that works together combining to resolve complex mathematical problems to verify new blocks. When registered, the data cannot be changed retroactively in any given block without modifying all subsequent blocks, which requires approval by the majority of the network.

Through Blockchain technology, one block forms every page in a transaction ledger. This block has a cryptographic hashing effect on the next block or tab. In other words, when a block is completed, it makes a special secure code, which ties in to another page or block, making a chain of squares or a blockchain.

B. Structure of Blockchain:

When a blockchain exchange flag has been lifted, a blockchain agreement must be achieved to change the similar in the network, with blocks linked by their respective hash codes to each other. Rather than relying on one 3rd party intermediate exchangeportion nodes inside the blockchain organize follow to a blockchain agreement convention to agree on the record substance and cryptographic hashes and progressed marks to ensure the cleverness of exchanges. These transactions in blockchain are considered effective and permanent once validated. Exchanges very much rely on the hash function with hash value. Such hash capacities are scientific forms that take input information of any measure, perform essential operations on it, and return a settled measure yield information. This hash feature makes them suitable for handling transactions. The final output would still be set and untampered, regardless of the size of the transactions. Beneath the hood of blockchains, hashing may be a component that naturally makes a difference to recognize between blocks.The hashing approach provides a unique identity for the blocks within a blockchain. Within a blockchain, blocks are theoretically known by the hashing which serves all identity and message authentication purposes. Public keys are provided by hashing functions. Here is an example of how to hash a bitcoin-blockchain. Blockchain provides the hash function SHA256 which produces a hash code of 256 bits.

IV. HASH FUNCTIONS

The hash algorithm is a deterministic method, projecting a hash input element in a much smaller set, from a larger set to an output element. Mapping the input element to a hash value. Hash functions can be defined as functions which transform any binary block Data into another binary block of a fixed size [1,2]. The result of an change Is known as Hash. The primary hash-function capacities It was suggested being used in sophisticated signature traditions with the aim of improving their productivity, since marks was built using data object digestion rather than total Components From a Machine perspective, hash capabilities are rendered utilized a principle of Trapdoor One-way Capacities (TOWF) specified by capability of both x and y set.

f: X!Y, with f(x) = y

Follows the following conditions:

1. F is symmetric feature, it has to be simple to calculate from a numerical point of view f (x) = y to both x2X components, yet instead it has to do the same time have been really challenging to procure *x = f1(y)* as y2Y provided.

2. When detailed information, defined as hidden door, is obtained, then measurement in polynomial time of Factor x2X This is f(x)=y.

A secure hash algorithm may then be symmetric job related to a variable size message m, Where even the msg has a position to some collection of msg, M, and gives a msg cycle with a decided, preordained bit scale, n. So The hash value, h, can be as described:

h : M!f0,1gn, with h(m)=bm

Because blockchain networks transform a msg of any duration through an n-bit sequence, the amount of bits that can be hashed is marginally smaller than the number of independent inputs. However there are still specific notifications that match the extracts.

PROPERTY TO:

The foregoing are essential properties to satisfy for these functions

1. Bit reliance: a hash code, *h(m)=bm*, requires to be cantered on a complex concept. The all message bits, instead if you alter a part of the message, the hash will also have to alter, Perhaps half of the parts, on. It enables data keenness to be assured, because it is outlandish to adjust any sum of bits, the result of the work will show up an mind blowing differentiate in between beginning hash as well as the unused hash, so test & screw up ambushes really aren't feasible.

2. Résistance to pre-image:

A notification m needs to be computationally hard to get, because of a hash *bm.* he *h(m)=bm*. To put it another way: every hash function since a theoretical Standpoint must be impossible toward undo. It is worth noting that the last two properties, despite being identical, are they're actually different.

3. Preimage moment resistance: Given a message m1, finding another message, m2, m1 6=m2, with the same hash must be computationally troublesome. This is to say, finding A further post *h(m1)=h(m2)* cannot be conceivable. This property considers some of the communications you want to identify then to identify a then seek to find another communication with almost same hash code.

4. Collision resistance: Discovering two messages m1 and *m2, m1 6= m2*, must be computationally alarming. So h*(m1)= h(m2).* The Communications are not subject to any requirements. Collision resistance could be a Weak state than momentary pre - image resistance based on the birthday catch 22. On the off chance of a hash work being Susceptible to crash tolerance, its usage is not necessary.

V. ELLIPTIC CURVES AND FINITE FIELDS.

Elliptic-curves:

An elliptic-curve has been spoken to type condition algebraically:

Y2=x3+ax+b for a=0 and b=7

(Bitcoin formula).

An elliptic-curve have essential assets. Eg: a non-vertical mark on the curve that crosses two non-tangent points may consistently cross. The 3rd argument planned the curve, either the frontal area at one level the property is non-vertical digression line to the curve should absolutely hit a different point upon its curve.

The attributes are utilized for establishing 2 operational activities: point-expansion as well as point-doubling.

The point-adding *(P+Q)=R*, generally thought of as a statement in line integrating P as well as Q along a third contact point x-axis is R'; Obtaining this using diagram is most straight forward.

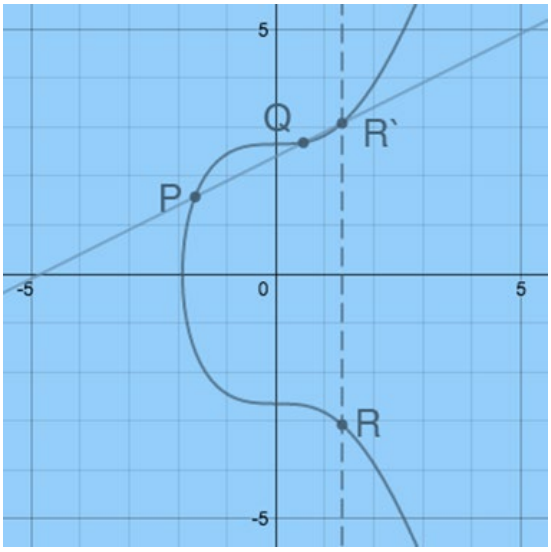

Fig. 2. Graph-Point of addition.

In addition, point multiplication, (P+P)=R the characterized find the tangent line to their point is increased, P focusing on a curve around the x-axis meet point dimension 'R'. Here's example of how it will feel as:

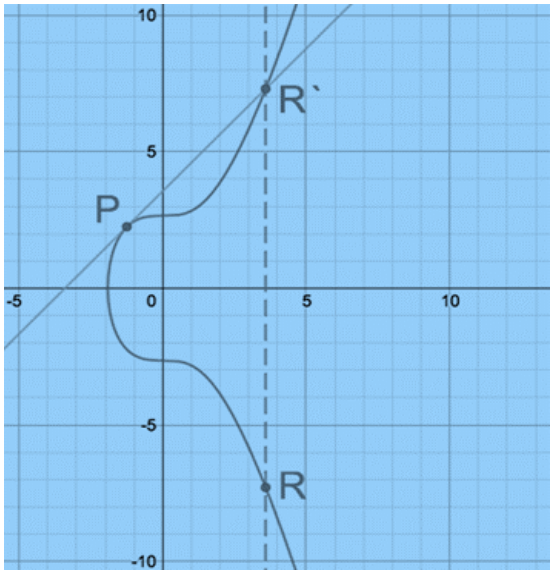

Fig. 3. Graph-Point of doubling.

These two operations are used together to multiply the scalar, R=aP, which is often described through applying a point dimension P to it's own.

R=7P

R=P+ (P+ (P+ (P+ (P+ (P+P)))))

A ratio increase approach the regularly rearranged via utilize of a combining point creation and level raise activities.

EXAMPLE: R=7P

R=P+6P

R=P+2(3P)

R=P+2(P+2P)

There, 7P was split down into 2 point multiplication steps then 2-point extension phases.

Finite Field:

The finite field may be thought of as a predefined set of +ve numbers inside ECDSA's setting from which each estimate has to drop. Some number "wraps through" outside that mark, so it falls under its cap.

The ideal method to ponder this is to calculate remainder, a described via the modulus (mod) functions. Eg, 9/7 donates 1 with 2 remaining:

9 mod 7 = 2

Our small sector here is Modulo 7, and therefore all mod activities in this region surrender the outcome that falls inside an expansion from 6.

VI. DIGITAL SIGNATURE

The digital signature is the technical process used an authorized document, a computer program or a computerized record being genuine and sensitive. As the advanced equivalent of a hand-written signature or stamped seal, a computerized signature provides much more characteristic protection and seeks to unravel the problem of modification and pantomime in advanced communications. A signature conspire must have a key generator that produces the combine of keys (sk, pk), the signature marking work S, and the signature confirmation work V. Here sk is the signer's mystery key and pk are the key for confirmation. The same secret key k is used for the signing and verification functions in a symmetric system, i.e. k = sk = pk. Sk is kept private by the signer in an asymmetric system, and pk may be published to everyone in public. Signature s is created to sign a message m by using s = Ssk(m). The message here is signature s. Vpk(m, z) is either true or false for any signature (i.e., message) z, namely.

$$V_{pk}(m,z) = \begin{cases} true & if\ z = V_{pk}(m) \\ false & otherwise \end{cases}$$

A message authentication system (or cryptographic communication system), private key or public key, is considered a good option for the signature scheme being implemented. The decryption feature is used as signing, and the encryption is used to verify:

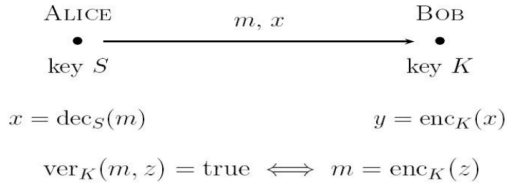

Fig. 4. Execution of a signature plot employing a cryptographic plot.

A public key encryption framework like RSA or ElGamal can be utilized. At that point Alice's key S is her secret key, which is used in communication mode for decryption, and Bob confirms the sign of Alice with her pub-key K.

To speak to the phases in every computerized signature arrangement, let's see how Alice, A, plans her Computerized identification identifier, m, is the private and available buttons, A and a, individually.

1. Alice can find the pub-key A, available for everyone who wishes to test their signature.

2. Simply chose the hash algorithm (h), Alice can determine its contract checklist to be signed, m, Using h. Decode communicates h(m) = bm.

3. In compliance with the encryption system E Hash, Alice will use its private key a to the file, get sign for file s: Ea (bm) = s.

4. Eventually, Alice will transmit the message 's sign has just been determined in accordance and the accompanying Signature: (m, s).

This procedure means Alice is post's signatory, because she is the only one who understands what his secret key is. If the recipient Bob, B, decides to check the Genuineness of A, authentication of msg m, accompanied by the corresponding code.

1. Evaluate text hash by utilizing its slimier hazing method used by Alice to get H(m)=for bm.

2. Decode with pub-key A, A, sign of a document, s, obtain: DA(s)=bm0=DA(Ea(bm)).

3. Finally, search to see if bm and bm0 values match. If so, then check the signature. Anyway, the

Signature is rejected for that post.

Additionally, previous procedure guarantees no message abuse during transmission. Since the value bm0 would otherwise not suit that of bm.

VII. ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA)

Throughout block-chain technologies, the signature schemes used most often are focused upon elliptic curves. The Digitalsignatures Procedure for the Elliptic-Curve (ECDSA) is a norm. The ECDSA (Elliptic-Curve Electronic Signature Algorithm), focused on cryptography using the elliptic curve (ECC), is a cryptographically secure digital signature scheme. ECDSA depends In this mathematics of cyclic bunches of elliptic-curve over small regions and the ECDLP problems. The ECDSA confirm an calculation is based on increase of EC focuses, and works as depicted underneath. The ECDSA key and marks for the same security standard are shorter than in RSA. A 256-bit ECDSA sign has the slimier level of protection as the RSA signing at 3072-bit. Defines elliptic-curve which are used in cryptographic:

- Generator G, used for the multiplication of scalar curves.

Harsh reality n of G-generated EC-points, indicating the duration of the private-key;

A. Core of Key Creation:

ECDSA Key-Pair consists of:

- Private key(integre) key: privKey
- Public key(EC): pubKey= privateKey* G

The Private Set Key [0 ... The n-1] is generated as a random integer The open key pubKey may be an elliptic curve point, determined through a replication of the EC point: pubKey=privKey*G.

- A EC main public point {x , y} can be compact to one of + 1 bit only (parity).

B. ECDSA Signature Creation:

The ECDSA sign algorithm takes A message msg + privKey as its origin and produces a signing comprising a pairs of {r, s} entries as output. The ECDSA signature algorithm is based on the ElGamal authentication protocol and will act while it continues:

1. Use of hash algorithm such as SHA-256to measure the hash message: ***h=hash(msg)***

2. Randomly generate the integer k throughout secure range***[1 .. N-1] N-1***

- The HMAC value k for deterministic-ECDSA is obtained from ***h + privateKey***

3. Evaluate the ***R=k*G*** also takings x co-ordinate: ***r=R.x***

4. Evaluate proof of the signature*:*

S= k-1(h+r privKey)(modn)k^{-1} * (h+r * privKey) \pmod nk-1(h+r privKey)(modn)

A turnaround measured k−1(mod n)k^{-1}pmod n k−1(mod n) is an numbers, such that k−11(mod n)k * k^{-1}equiv 1pmod n k−1(mod n) is an numbers.

5. Return signature{r, s}.

A {r, s} signature defined has been a set of records, every inside the range of [1] N-1). The random point R = k*G is encoded along with a statement s, showing the both message h and privKey are identified by the verifier. The proof s can be verified with the respective public Key.

The ECDSA identifiers was Two times greater than the secret key used by the signer for the curve during the authorization process.

C. ECDSA Signature Verification:

The ECDSA signature verification algorithm take a message labelled msg + a sign {r, s} as input made as of marking calculation adding public key, which compares the secret key of underwriter. The result is Boolean: Signature true (or) false. An ECDSA sign verifies as the following workings of the algorithm (with slight assumptions):

1. Evaluate the hash message, using Similar strong cryptographic algorithm used throughout the process of sign : ***h= hash (msg)***

2. Evaluate proof of universal inverse signature:

S1 = s-1 (mod n) s^ {-1} \pmod n s-1 (mod n)

3. Restore a subjective point used during signature:

R`=(h *s1) * G+(r*s1)*

4. Consider R 'x-coordinate: **r'=R'.x**

5. Verify the given result of the sign confirmation via comparison.

The basic principle of the signature authentication is to use the public key to recover point R 'and to verify If it is the same point R, automatically updated mostly during sign cycle.

D. ECDSA working:

Easy reason for the ECDSA signature {r, s} is:

The marking marking encodes an arbitrary point R Via elliptic-curve modifications utilize a secret-key Private-Key as well as the hash h response to an integer s, which is a guarantee that the private key privKey is identified to the underwriter. Due to the ECDLP issue the signature {r, s} cannot reveal the private key.

The sign authentication uses the cryptographic key pub-Key and the message hash h to decipher the proof number s from the signature back to its original point R, and compares the x-coordinate of the obtained R with the signing value r.

E. Signal Assessment:

Calculated during the signature test, the equation behind point R' recovery Can be converted as follows replace publicKey with privateKey*G:

R`=(h *s1) * G+(r*s1)*pubkey== **(h *s1) * G+(r*s1)* privkey*G==(h+r*=privKey)*s1*G**

When glance at the count

S1 = s-1 (mod n) s^ {-1} \pmod ns-1 (mod n) like this: **S1 = s-1 (mod n) s^ {-1} \pmod ns-1 (mod n)== (k-1(h+r privKey)(modn)k*{-1} * (h+r * privKey) {^-1}\pmod nk(h+r privKey)-1 (modn)**

Know, substitute point R' with s1.

R`=(h+r * privKey)*s1*G=(h+r privKey) k(h+r privKey)-1 (modn) (h+r * privKey)* k * (h+r privKey)^{-1}\ pmod n(h+r privKey) k(h+r privKey)-1(modn) * G=k * G * G * privKey (h+r * privKey)

The last step is to compare R' with R'. Therefore, the algorithm contrasts R' and R" x co-ordinates only: r' and r variable.

R'==r is expected if the symbol is correct and Where the secret key or signature is wrong, r' r' r is projected.

In the sense of a finite field, ECDSA uses elliptic curves that change their presence considerably though not the fundamental conditions or one of a kind properties. The similar condition with in limited arena of mod 67 plotted above, it is also a set of numbers at present, where all x and y values are inerrable between and 66. Remember their horizontal symmetry is also maintained by the "curve".

Point expansion and multiplying are presently marginally distinctive Visibly. Lines traced on this graph should wind around the vertical and even directions, similar to a diversion-of Space rocks, keeping up the same slant. So including focuses (2, 22) and (6, 25) looks like this:

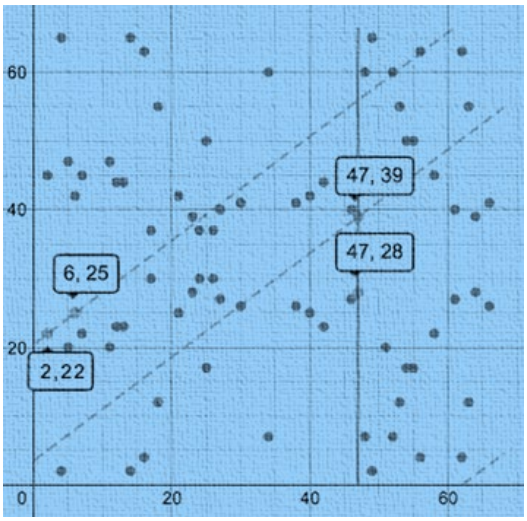

Fig. 5. Graph-Point of addition on Finite Field.

ECDSA is the basis of how the implementations for Bitcoin as well as other blockchains operate. The system has withstood some very rigorous statistical and analytical checking of vulnerabilities. The few errors that took place in practice were usually attributed to users not being cautious to secure their private keys, or using a relatively Easy generator of pseudorandom numbers to generate privt-key which attackers may misuse.

VIII. BITCOIN AND ECDSA

A rule like Bitcoin chooses a range of elliptic-curve parameters and their n number of arena representation which is unchanged for all rules implementations. A factor provide the structure utilized, the area's primary factor and the curve's base point. The starting assumption value, that is not specified separately and could be a portion of different criteria, could be expressed mathematically as either the number of times that argument may be used in itself before its slant is infinite or as a longitudinal thread. An initial point is selected since the arrangement could have been a huge positive integer.

For its starting level, prime modulo, and order, Bitcoin uses a very big numbers. All realistic ECDSA implementations currently use big values. The algorithm 's reliability is dependent on such values being high, and thus Let brute force or reversed design inefficiency.

Regarding the situation at Bitcoin:

Equation Ellipric Curve: y2=x3+7

Prime mogulo= 2^256-2^32-2^9-2^8-2^7-2^6-2^4-1=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFC2F

Basepoint=0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798 483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A6855419 9C47D08F FB10D4B8

Order=FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFE BAAEDCE6 AF48A03BBFD25E8CD0364141

Any work as well as a considerable value to anticipation involve a discovery with correct criteria. It seems, a maybe, seemingly odd amount might mask the plan to reconstruct the secret key behind the backdoor. As short, such unique discovery is called sep256k1 as well as it seems to be actually a series of elliptic curve structures over narrow areas that are recommended to cryptographic usage.

IX. CONCLUSION AND ENHANCEMENTS

The most cryptographic instruments contributing to the protection and unwavering consistency of blockchain are demonstrated in this work: Hash-capacities, advanced marks, elliptic-curve. We learn how Blockchain technology functions profoundly. In this article specified a class of mathematics behind the working of Blockchain. Have established a certain intuition of the deep mathematical connection between public-key also private-key. We have shown how intelligent implementation for the easiest mathematics methods will establish its one-way "locked door" Functionality needed to maintain information asymmetry that differentiates bitcoin ownership. ECDSA is the basis of how the implementations for Bitcoin and other blockchains operate. The system has withstood some very rigorous statistical and analytical checking of vulnerabilities.

REFERENCES

[1] Menezes, A.J.; van Oorschot, P.C.; Vanstone, S.A. Handbook of Applied Cryptography; CRC Press, Inc.:
Boca Raton, FL, USA, 1996. [CrossRef]

[2] Paar, C.; Pelzl, J. Understanding Cryptography. A Textbook for Students and Practitioners; Springer: Heidelberg, Germany, 2010. [CrossRef].

[3] Review Analysis of the Cryptographic Tools for Blockchain and Bitcoin Víctor Gayoso Martínez , Luis Hernández-Álvarez and Luis Hernández Encinas * 10 December 2019; Accepted: 11 January 2020; Published: 15 January 2020.

[4] Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto satoshin@gmx.com www.bitcoin.org.

[5] Potentials of Blockchain Technology for Construction Management Žiga Turka,* and Robert Klincb Creative Construction Conference 2017, CCC 2017, 19-22 June 2017, Primosten, Croatia ScienceDirect Available online at www.sciencedirect.com

[6] Blockchain Technology : Classification, Opportunities, and Challenges Nadir Abdelrahman Ahmed Farah International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056

[7] Conceptualizing blockchains: characteristics & applications karim sultan1, Umar Ruhi1 and Rubina Lakhani2 11th IADIS International Conference Information Systems 2018

[8] An Overview of Blockchain Technology:Architecture, Consensus, and Future Trends

[9] Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3 2017 IEEE 6th International Congress on Big Data

[10] https://cryptobook.nakov.com/digital-signatures/ecdsa-sign-verify-messages

[11] Implementation of Elliptic Curve Digital Signature Algorithm Aqeel Khalique Kuldip Singh Sandeep Sood International Journal of Computer Applications (0975 – 8887)Volume 2 – No.2, May 2015

[12] https://medium.com/dataseries/explaining-the-math-behind-blockchain-algorithms

[13] https://www.coindesk.com/math-behind-bitcoin